# MICROCOMPUTER SECURITY 6241

<span style="color:red">(May 2003)</span>

## Responsibility

**Division Chief**

Conservation camp staff use computers in their daily operations for word processing, data management, and electronic communications with the wide area network system. It is essential that the security of the camp or institution be maintained and that no unauthorized communication by computer to another computer or electronic device is made. It is also very important to maintain data integrity and systems security for the computer systems located in the work setting.

**All**

To help maintain system security and minimize potential risks, the following procedures shall be followed when utilizing wards to perform data entry:

1. A ward may not have a computer, modem, or terminal in his/her possession within the camp.

2. There shall be no ward access to a computer outside the ward's authorized work area or school.

3. No ward shall be permitted access to any computer unless the ward is under specific supervision of staff member.

4. Ward access to computers will be in compliance with Institutions and Camp policy on computer use.

5. Wards shall not have access to any computer containing sensitive or confidential information. Documents containing employee information such as addresses, telephone numbers, Social Security Account Numbers, credit card numbers, driver's license numbers, or any other form of personal information shall not be stored in computers accessible to wards.

6. Wards shall not be permitted to possess any tool (such as screwdrivers, pliers, wrenches, files, etc.) while working on, or near any computer.

The Camp Division Chief and Camp Superintendent shall develop a local procedure for computer security including; responsibilities of camp staff for assuring computer security, positive key control for any keys which unlock keyboards or CPU cases, storage of computer backup diskettes, and security requirements for each specific computer and computer work area.